Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A method for detecting spam in a messaging system comprising:

generating a white list of confirmed message senders, each of said confirmed message senders being authorized to send ~~having been confirmed as being able to receive~~ messages as evidenced by prior receipt of a response to a confirmation message;

sharing the white list among a plurality of spam filters in the messaging system;

using the white list at a given one of the plurality of spam filters to determine if a sender of a received message has been previously confirmed;[[,]] and

~~if so,~~ forwarding the received message to a recipient without separately confirming the sender if it is determined that the sender has been previously confirmed.

2. (Currently amended) The method of claim 1 wherein the messaging system is an email system.

3. (Currently amended) The method of claim 1 wherein sharing the white list includes sharing the white list ~~is shared~~ with at least two spam filters.

4. (Currently amended) The method of claim 1 wherein if the sender has not been previously confirmed, the method further includes:

sending a confirmation to the sender;[[,]]

verifying a response from the sender;[[,]] and

if the response is verified, adding the sender to the white list at the given spam filter and

sharing the information associated with the added sender with other spam filters in the messaging system.

5. (Original) The method of claim 1 wherein sharing includes publishing the white list at a central location.

6. (Currently amended) The method of claim 1 further comprising maintaining the white list at a central location, wherein using the white list includes checking the white list maintained at the [[a]] central location.

7. (Currently amended) The method of claim 1 wherein ~~the~~ if the sender has not been previously confirmed, the method further comprising: ~~including~~

sending a confirmation to sender;[[,]]

verifying a response from the sender;[[,]] and

if the response is verified, adding the sender to the white list maintained at a central location that is shared among the plurality of spam filters.

8. (Currently amended) A method for identifying a spam message comprising:

receiving a message at a spam filter in a network that includes a plurality of spam filters, each spam filter having an associated list of confirmed senders;

identifying a ~~the~~ sender of the message;

determining if the sender has been previously confirmed as a confirmed ~~valid~~ sender including:

determining if the sender is included in a list of confirmed senders ~~for~~ associated with at least one ~~any~~ spam filter in the network;

if it is determined that the sender is not included in the list of confirmed senders associated with the at least one spam filter, determining if the sender is included in a list of confirmed senders associated with another one of a plurality of spam filters; and

if it is determined that the sender is included in a list of confirmed senders associated with any one of the spam filters[[so]], then forwarding the received message to a recipient without separately confirming the sender in each spam filter.

9. (Original) The method of claim 8 wherein the message is an email message.

10. (Currently amended) The method of claim 8 further comprising sharing a ~~wherein the white~~ list of confirmed senders associated with one spam filter with another spam filter ~~is shared with at least two spam filters~~.

11. (Currently amended) The method of claim 8, wherein if it is determined that ~~further comprising: determining if~~ the sender has not been previously confirmed ~~and if not confirmed~~, the method further comprising:

sending a confirmation to the sender;[[,]]

verifying a response from the sender;[[,]] and

if the response is acceptable, adding the sender to the ~~white~~ list of confirmed senders at an associated ~~the given~~ spam filter and sharing information with other spam filters in the network, the information including information indicating that the sender has been confirmed.

12. (Currently Amended) The method of claim 11 wherein sharing information with other spam filters includes publishing the ~~white~~ list of confirmed senders at a central location that can be accessed by the spam filters.

13. (Currently Amended) The method of claim 8 [[11]] further comprising maintaining each ~~wherein determining includes checking a white~~ list of confirmed senders ~~maintained~~ at a central location, wherein determining if the sender has been previously confirmed includes checking at least one list of confirmed senders at the central location.

14. (Currently Amended) The method of claim 8 [[13]], wherein ~~further comprising~~ if the sender has not been previously confirmed, the method further comprising:

sending a confirmation to the sender;[[,]]

verifying a response;[[,]] and

if the response is acceptable, adding the sender to the ~~white~~ list shared among the plurality of spam filters.

15. (Currently amended) A method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising:

collecting information relating to a sender from a plurality of the spam filters;[[:]]

determining a trend in the collected information; and

identifying ~~identify~~ a spammer based on the trend.

16. (Original) The method of claim 15 wherein collecting information includes collecting information relating to a number of messages sent by a sender to unrelated email addresses.

17. (Original) The method of claim 15 wherein determining trends includes correlating the messages received by an individual spam filter relating to a same sender.

18. (Currently amended) The method of claim 15 wherein identifying includes determining that a sender is a spammer if a number of messages sent to unrelated email addresses ~~in the correlated data~~ exceeds a predetermined threshold.

19. (Original) The method of claim 18 wherein the threshold is time dependent.

20. (Currently amended) A method for detecting spam in a messaging system comprising:

generating a ~~white~~ list of confirmed message senders and maintaining the ~~white~~ list at a data center;[[:]]

receiving a message at a spam filter in a network that includes a plurality of spam filters;[[:]]

verifying with the data center that a [[the]] sender of the message is a confirmed message sender, and [[add]]

if it is determined that the sender is a confirmed message sender [[so]], forwarding the received message to a recipient without separately confirming the sender.

21. (Original) The method of claim 20 wherein the message is an email message.

22. (Currently amended) The method of claim 20 further comprising sharing the ~~white~~ list with at least two spam filters in the network.

23. (Currently amended) The method of claim 20 wherein if it is determined that the sender is not a confirmed message sender, the method further comprising: ~~determining if the sender has not been previously confirmed, and if not confirmed then~~

sending, from the data center, a confirmation to the sender;[[,]]

verifying a response received at the data center from the sender;[[,]] and

if the response is acceptable, adding to the ~~white~~ list of confirmed message senders a name associated with ~~identifying~~ the sender; and

sharing information including the name ~~identifying the sender as being confirmed~~ with other spam filters in the network.

24. (Currently amended) A method for identifying a spam message comprising:

receiving a message at a spam filter in a network that includes a plurality of spam filters;

identifying a ~~the~~ sender of the message;

verifying, at ~~with~~ a data center coupled to ~~a plurality of~~ the spam filters, [[if]] the sender

has been previously confirmed as a confirmed ~~valid~~ sender including determining if the sender is included in a list of confirmed senders ~~for~~ associated with at least one ~~any~~ spam filter in the network, the ~~said~~ list being maintained at the data center; and

if the sender has been previously confirmed, forwarding the received message to a recipient without separately confirming the sender.

25. (Original) The method of claim 24 wherein the message is an email message.

26. (Currently amended) The method of claim 24 further comprising sharing a ~~wherein the~~ list of confirmed senders associated with one spam filter with another spam filter ~~is shared with at least two spam filters~~.

27. (Currently amended) The method of claim 24 wherein if the sender has not been previously confirmed, the method further comprising: ~~determining if the sender has not been previously confirmed, and if not confirmed~~

sending, from the data center, a confirmation to the sender;[[,]]

verifying a ~~if the~~ response from the sender is acceptable;[[,]] and

adding a [[an]] name identifying the sender to the list maintained at the data center.

28. (Currently amended) A method for detecting a spammer in a network that includes a plurality of spam filters, the method comprising:

collecting, using a data center, information relating to a sender from a plurality of the spam filters;[[:]]

determining a trend in the collected information; and

identifying ~~identify~~ the sender as a spammer based on the trend[[,]] including adding the sender to a list of confirmed spammers maintained by the data center.

29. (Currently amended) The method of claim 28 wherein collecting information

includes collecting information relating to a number of messages sent by the [[a]] sender to unrelated email addresses.

30. (Original) The method of claim 28 wherein determining trends includes correlating messages received by an individual spam filter relating to a same sender.

31. (Currently amended) The method of claim 28 wherein identifying the sender as a spammer includes determining that the [[a]] sender is a spammer if a number of messages sent to unrelated email addresses ~~in the correlated data~~ exceeds a predetermined threshold.

32. (Original) The method of claim 31 wherein the threshold is time dependent.

33. (Currently amended) A method for filtering spam in a messaging system comprising:

confirming that a message sender can receive one or more messages;

sharing information indicating that the message sender can receive one or more messages among a plurality of spam filters in the messaging system;

using said information at a given one of the plurality of spam filters to determine if a message should be sent to an intended recipient ~~allowed~~ without separately determining whether the message sender can receive one or more messages.

34. (Original) The method of claim 33 wherein the message is an email message.

35. (Original) The method of claim 33 further comprising confirming at a first spam filter in the system that a sender of a message can receive messages.

36. (Original) The method of claim 35 further comprising receiving the message at a second spam filter.

37. (Original) The method of claim 35 further comprising sharing information developed by the first spam filter with one or more other spam filters in the messaging system.

38. (Original) The method of claim 37 further comprising sharing the information with a data center, and thereafter allowing access by each of the spam filters in the messaging system to the information.

39. (Currently amended) The method of claim 33 wherein the information is maintained in a list that includes one or more ~~of~~ confirmed message senders.

40. (Original) The method of claim 39 wherein the list is shared with a plurality of the spam filters in the messaging system.

41. (Currently amended) The method of claim 39 wherein the ~~information is maintained in a~~ list ~~which~~ is maintained by a data center accessible by the ~~a plurality of~~ spam filters in the messaging system.

42. (Original) The method of claim 41 further comprising sharing the list with a plurality of spam filters in the messaging system.

43. (Currently amended) The method of claim 42 further comprising maintaining a copy of the list at one or more of the ~~a plurality of~~ spam filters in the messaging system.

44. (Currently amended) The method of claim 39 further comprising:

associating a passcode with one or more of the confirmed senders in the list;[[,]] and

verifying a message received from a sender in the list including verifying ~~includes~~ the passcode [[if]] specified by the sender.

45. (Currently amended) The method of claim 44 further comprising prompting ~~triggering an addition of a passcode for~~ a sender in the list to enter a passcode upon an occurrence of an predefined event.

46. (Currently amended) The method of claim 45 further comprising detecting ~~wherein the event includes detection~~ that an email address associated with the sender has been compromised, and

prompting the sender to enter the passcode thereafter.

47. (Currently amended) The method of claim 39 further comprising:

receiving ~~including~~ a pass code from the ~~in the list for each~~ confirmed message sender; and

verifying the pass code is included in the message prior to forwarding the message from the confirmed message sender to the intended [[a]] recipient.

48. (Original) The method of claim 47 further comprising automatically adding the passcode associated with the sender at a time for transmission of a message from the sender in the messaging system.

49. (Currently amended) The method of claim 48 further comprising providing a plug-in ~~plug-in~~ module for automatically adding the passcode, the plug-in ~~plug-in~~ module adapted to add the passcode prior to transmission to the messaging system.

50. (Original) The method of claim 33 further comprising:

correlating sender-recipient data at a spam filter in the messaging system and determining data related to how fast a list of recipients grows for a given sender;

determining a list of unacceptable senders using the sender-recipient data and the determined data; and

sharing the list of unacceptable senders with other spam filters in the messaging system.

51. (Original) The method of claim 50 further comprising maintaining a list of recipients for each sender of messages processed by a given spam filter.

52. (Original) The method of claim 51 further comprising maintaining the list of recipients for each sender at a data center.

53. (Currently amended) A method for processing messages at a spam filter in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a message for processing, the message from a [[an]] sender for delivery to an intended recipient;

determining if the sender is a confirmed sender[[,]] including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the ~~plurality of~~ spam filters in the messaging system, where confirmed senders are senders having a verified capability to receive messages; and

if it is determined that the sender is a confirmed sender, enabling transmission of the message to the intended recipient.

54. (Currently amended) A method for processing messages at a spam filter in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a message for processing, the message from a sender for delivery to an intended recipient;

determining if the sender is a confirmed sender, including querying a data center to determine if the sender is included in a list of confirmed senders based on information received from any of the ~~plurality of~~ spam filters in the messaging system, where confirmed senders are

senders having a verified capability to receive messages;

if it is determined that the sender is a not a confirmed sender, confirming the sender including sending the sender a notification; and

upon receipt of a confirmation from the sender in response to the notification, sharing the sender's confirmed status with the plurality of spam filters in the messaging system including publishing the sender's status to the data center.

55. (Currently amended) A method for minimizing spam in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages;

evaluating a list of confirmed senders; and

providing a notification to the one spam filter indicating whether the sender's status is confirmed.

56. (Currently amended) A method for minimizing spam in a messaging system, the messaging system including a plurality of spam filters, the method comprising:

receiving a request from one of the spam filters in the messaging system to verify if a sender of a message is a confirmed sender, a confirmed sender being a sender having a verified capability to receive messages;

evaluating a list of confirmed senders;

if the sender is not included in the list of confirmed senders, confirming the sender including providing a notification to the sender; ~~and~~

upon receipt of a confirmation from the sender in response to the notification, sharing the sender's status with ~~the~~ other spam filters in the messaging system including adding the sender to the list; and

notifying ~~providing a notification to~~ the one spam filter indicating whether the sender's

status is confirmed.

57. (Original) The method of claim 56 wherein the step of confirming the sender is performed by a spam filter.

58. (Original) The method of claim 56 wherein the step of confirming the sender is performed by the requesting spam filter.